CYBERSECURITY FOR BUSINESSES
SDPD Crime Prevention
April 5, 2016

CONTENTS

Cyber crimes involve the illegal use of or the unauthorized entry into a computer system to tamper, interfere, damage, or manipulate the system or information stored in it. Computers, including mobile devices, can be the subject of the crime, the tool of the crime, or the target of the crime.

As the subject of a crime, a criminal would use your computer or another computer to willfully alter the information stored in your computer, add fraudulent or inaccurate information, delete information, etc. Motives for this include revenge, protest, competitive advantage, and ransom.

As the tool of a crime, a criminal would use a computer to gain access to or alter information stored on another computer. In one common mode of attack a hacker would send a "spear phishing" e-mail to employees who have access to the business bank account. The e-mail would contain an infected file or a link to a malicious website. If an employee opens the attachment or goes to the website, malware or malicious software that gives the hacker access bank account log-ins and passwords would be installed on the computer. The hacker would then have electronic payments made to accounts from which the money would be withdrawn. Criminals also use computers to commit various frauds and steal identities and other information.

As the target of a crime, computers and information stored in them can be stolen, sabotaged, or destroyed. Trade secrets and sensitive business information stored in computers can be lost in these kinds of attacks.

If you answer "no" to any of the following questions you need to worry about your cybersecurity and you should take appropriate steps to get to "yes."

Do we know what's connected to our network?
Do we know what's running or trying to run on our networks?
Do we properly manage the people who have administrative permission to wander around our network?
Do we have an automatic system that continuously monitors our network?

Your computers and the information in them should be protected as any valuable business asset. The tips in this paper suggest various physical, procedural, and operational protective measures that can be employed in dealing with malware, bank accounts, social media, mobile devices, Wi-Fi hacking, Internet use, data breaches, and business activities. For more details see National Institute of Standards and Technology (NIST) Interagency Report NISTIR 7621 entitled *Small Business Information Security: The Fundamentals*. A revised draft dated December 2014 is available online at **http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf**. It and many other reports are available online under NIST IR Publications on **http://csrc.nist.gov**.

Also, consider joining the FBI's InfraGard, a partnership with the private sector with the goal of promoting an ongoing dialogue and timely communications between its members and the FBI. Its members gain access to information that enables them to protect their assets from cyber crimes and other threats by sharing information and intelligence. Go to **www.infragard.net** to apply for membership.

PHYSICAL PROTECTIVE MEASURES

- Don't allow unauthorized persons to have access to any of your computers. This includes cleaning crews and computer repair persons.
- Install surface or cable locks to prevent computer equipment theft.
- Install computers on shelves that can be rolled into lockable furniture when employees leave their work areas.
- Locate the computer room and data storage library away from outside windows and walls to prevent damage from external events.
- Install strong doors and locks to the computer room to prevent equipment theft and tampering.
- Reinforce interior walls to prevent break-ins. Extend interior walls to the true ceiling.
- Restrict access to computer facilities to authorized personnel. Require personnel to wear distinct, color-coded security badges in the computer center. Allow access through a single entrance. Other doors should be alarmed and used only as emergency exits.

SPECIAL MEASURES FOR LAPTOPS

Special security measures are needed for laptops to prevent them from being stolen and the data in them used to harm your business.

- Train employees in the need for special measures to protect laptops and their data wherever they may be used.
- Issue desktops instead of laptops to employees who seldom leave their offices.
- Have employees lock up their laptops when they are left unattended in their offices. Laptops should never be left unguarded.
- Have employees carry their laptops in a sports bag or briefcase instead of the manufacturer's bag.
- Don't leave a laptop visible inside vehicles or unattended in public places.
- If left unattended, secure the laptop with a cable lock to something that cannot be easily moved. Or install an alarm that will sound if the laptop is moved.
- Create a loss response team to monitor compliance with laptop and data security measures, investigate losses, assess data needs, and remove data no longer needed.

The following measures should be employed to protect your business in the event a laptop is lost or stolen.

- Have employees back up their files so they can be recovered if their laptop is lost or stolen. These back-up files should be kept in a separate, secure place.
- Protect data with strong passwords, i.e., ones that are at least 12 characters long, completely random, and have at least one capital letter, one lowercase letter, one number, and one symbol.
- Don't store passwords on laptops.
- Determine if employees need all the data on their laptops to perform their jobs. Remove any data that is not needed.
- Encrypt all sensitive information so it cannot be compromised.
- Install software that will enable you to erase sensitive information when the thief logs onto the Internet.

The following measures can help you recover a laptop that has been lost or stolen.

- Keep a record of all laptop model and serial numbers so if one is recovered you can prove it is yours. Also keep the sales receipt and register the laptop with the manufacturer.
- Place stickers on the laptops with a phone number to call if one is lost and found by an honest person. But don't put the business name on it. That could be used by criminals to guess passwords or assess the sensitivity of the data stored on the laptop.
- Install hardware, software, or both to aid in recovery of the laptop. After you report the laptop lost or stolen the software enables a monitoring company to track the laptop when the thief logs onto the Internet. Hardware systems work the same but have a Global Positioning System (GPS) device that can pinpoint its location.
- Report the loss to the local law enforcement agency, and notify the manufacturer.
- Look for it on Craigslist and E-Bay.

PROCEDURAL AND OPERATIONAL PROTECTIVE MEASURES

- Classify information into categories based on importance and confidentiality. Use labels such as "Confidential" and "Sensitive." Identify software, programs, and data files that need special access controls.
- Limit employee access to what he or she needs to do their job. Review this periodically. No employee should have unlimited access, especially to personally identifiable information.
- Require two people to be involved implementing measures to protect or serve your network.
- Reevaluate the access needs of those in senior and supervisory positions as they are promoted.
- Clearly document and consistently enforce all policies and controls.
- Install software-access control mechanisms. Require a unique, verifiable form of identification, such as a user code, or secret password for each user. Install special access controls, such as a call-back procedure, if you allow access through a landline connection.
- Have your Information Technology (IT) manager change the administrative password on a regular basis. A number of free tools are available for this if manual modification is not practical. This password should also be changed during non-business hours.
- If warranted, hire a dedicated information security officer. It has been suggested that companies with this officer detect more security incidents and report lower financial losses per incident that those without one.
- Require that passwords be changed at least every three months and not be shared, i.e., used for different logins. Employees should have a unique password for each system and service they use. There are many password management tools available that can help with this process.
- Employee user accounts should not have administrative privileges. This will prevent the installation of any unauthorized software or malicious code that an employee might activate.
- Change security passwords to block access by employees who change jobs, leave, or are fired. The latter become a high risk to your business for revenge or theft.
- Encrypt confidential data stored in computers and mobile devices, or transmitted by e-mail or over communication networks. Use NIST data encryption standards.
- Design audit trails into your computer applications. Log all access to computer resources with unique user identification. Separate the duties of systems programmers, application programmers, and computer programmers.

- Review automated audit information and control reports to determine if there have been repeated, unsuccessful attempts to log-on both from within and outside your facility. Look for unauthorized changes to programs and data files periodically.
- Use monitoring or forensic tools to track the behavior of employees suspected of malicious activities. Cyber crimes committed by malicious employees are among the most serious threats to networked systems and data. They can disrupt operations, corrupt data, exfiltrate sensitive information, or compromise an IT system. For more information on insider threats and how to prevent fraud see the *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* published by the Carnegie Mellon University and Software Engineering Institute, July 2012. It can be downloaded at **www.sei.cmu.edu/reports/12sr004.pdf.**
- Pay closer attention to those in special positions of trust and authority, e.g. accountants and managers, because it is easier for them to commit high-value crimes.
- Monitor incoming Internet traffic for signs of security breaches.
- Make backup copies of important business information, i.e., documents, spreadsheets, databases, files, etc. from each computer used in your business. This is necessary because computers die, hard disks fail, employees make mistakes, malicious programs can destroy data, etc. Make backups automatically at least once a week if possible. Make a full backup once a month and store it in a protected place away from your business.
- Review and test data backup procedures periodically to ensure that business information has been backed up and is capable of being fully restored. Remember that some variants of ransomware will encrypt network data so it's important to segregate backup systems from your primary network.
- Delete all information stored in your printers, copiers, and fax machines at least once a week. Use a secure data deletion program that will electronically wipe your hard drives. Simply hitting the delete key will leave some data on the hard drive.
- Be careful in getting outside help with computer security problems. Call the San Diego District Office of the U.S. Small Business Administration at **(619) 727-4883** for advice and recommendations. Start with a list of vendors or consultants. Then define the problem, send out a request for quotes, examine each quote, and check the provider's references and history before hiring one.
- If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Crime Center NW3C, at **www.ic3.gov**. The IC3 website also includes tips to assist you avoiding a variety of Internet frauds.
- Beware of the Business E-mail Compromise (BEC) cam or CEO fraud if your business works with foreign suppliers or regularly makes wire-transfer payments. In one version of this scam the e-mail account of a high-level executive is compromised and a request for a wire transfer to the scammer's account is made from it to the employee responsible for wiring money to overseas banks. In April 2016 the FBI warned about a dramatic increase in these scams and estimated that they scams have cost organizations more than $2.3 billion in losses over the past three years. For more information on BEC scams see FBI Public Service Announcement, Alert No. I-012215-PSA dated Jan. 22, 2015 at **www.ic3.gov/media/2015/150122.aspx**. The IC3 suggests the following measures to help protect you and your business from becoming victims of a BEC scam.
    - Avoid free, web-based e-mail. Establish a business website domain and use it to establish business e-mail accounts.
    - Be careful what is posted to social media and business websites, especially job duties and descriptions, hierarchal information, and out of office details.
    - Be suspicious of requests for secrecy or pressure to take action quickly.
    - Consider additional IT and financial security procedures and Two-Factor Authentication (TFA), for example: verify significant transactions with telephone calls, use digital signatures, delete e-mail from unknown parties without opening it or attachments or clicking on links in it, and use Forward instead of Reply to respond to any business e-mails with the correct e-mail address typed in or selected from your e-mail address book to ensure the intended recipient's correct e-mail address is used.
    - Beware of sudden changes in business practices, e.g., if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been on a business e-mail.
    - Always verify via other channels that you use with a legitimate business partner.
- Develop a response plan to control the damage that can result from malicious insider activity. The response team would assist in investigating the fraud and use the lessons learned to prevent further fraud and improve the plan.

- Install a quality spam filter. The majority of cyberattacks and phishing attempts come through e-mail, and simply keeping spam out of your network can greatly reduce your risk.
- Protect your employees from receiving malicious e-mail. With access to all incoming e-mail and knowledge of the kinds of e-mail that each employee normally receives, a security system could recognize unusual e-mail and warn employees of it. It could also warn of e-mail that requests employees to open attachments, verify passwords, or go to another website.

PREVENTING INSIDER VISUAL HACKING

Conduct a visual privacy audit to determine your organization's vulnerability to insider visual hacking, i.e., where someone within your organization obtains or captures sensitive information for unauthorized use, e.g., by taking photos of documents left on a printer or information displayed on a screen, or simply writing down employee log-in information that is taped to a computer monitor. The hackers could be employees, contractors or service vendors such as cleaning and maintenance crews, and visitors. Here are some questions to ask in the audit.

- Does your organization have a visual privacy policy?
- Are shredders located near copiers, printers, and desks where confidential documents are regularly handled?
- Are computer screens angled away from high-traffic areas and windows, and fitted with privacy filters?
- Do employees keep log-in and password information posted at their workstations or elsewhere?
- Are employees leaving computer screens on or documents out in the open when not at their desks?
- Do employees know to be mindful of who is on the premises and what they are accessing, photographing, or viewing?
- Are there ways to report suspicious activities?

One result of this audit may be the adoption of a "clean desk" policy that would require employees to do the following.

- Turn device screens off and remove all papers from your desk when leaving them unattended.
- Use a password-protected screensaver.
- Memorize passwords or keep them locked up. Don't put them on sticky notes or pieces of paper on your device or desk.
- Lock desks, filing cabinets, and office door at the end of the work day.
- Lock up mobile devices, including laptops, tablets, smartphones, PDAs, CD/DVD discs, and USB drives, when not in use.

Other measures to help defend against visual hackers include the following.

- Mask high-risk data applications to onlookers using strategies from most to least secure.
- Make shredders standard issue to all offices. Locate them near copiers, printers, and fax machines. Make their use a prerequisite for those who telework or have remote network access to corporate information.
- Install privacy filters on all computers and electronic devices use in and out of the office. Privacy filters blacken out the angled view of onlookers while providing an undisturbed viewing for the user. They can be fitted to the screens of desktop monitors, laptops, and mobile devices.

The growing problem of insider threats shouldn't instill fear or suspicion in employees about the people they see and talk to every day. However, they should be made aware of the reality of the threat and the role they play in protecting the organization's sensitive data, including that of its customers and clients. You should also carry out periodic inspections, rectify any violations found, cite employees for them, and keep a record of violations and provide additional training as necessary.

MITIGATING THIRD-PARTY VENDOR THREATS

There are myriad security risks in giving third-party vendors access to your network and data. If a third party gets hacked, your company can lose vital business data and confidential employee information can be compromised. If it's a serious hack, the consequences for your company can range from white-hot media attention to a damaged reputation, lawsuit hell, higher insurance costs, extensive financial loss and even bankruptcy. Some of the most devastating breaches in the past few years have been rooted in the security weaknesses of third parties, and in fact, hackers themselves admit that contractors are often their primary target. The Target breach in 2013 is a case in point. It exposed about 40 million debit and credit card accounts. The initial intrusion into Target's systems was traced back to network credentials stolen from a third-party HVAC vendor. A study after that found that 63 pecent of data braches were linked to a third-party vendor that was responsible for system support, development, and/or maintenance. In some cases, the victimized companies did not even know that a third party handled certain security functions.

As networks grow to include partners, contractors, outside service providers, and third-party vendors, it becomes harder for a business to manage and protect its assets. Businesses must be able to visualize and understand their network's traffic and users, and in turn the risks to their systems. Recognizing risk is central to securing your network. You need to know who your network users are, when and why they are accessing your network, and what they are doing inside it. You need to understand how they are interacting with your network and sensitive information so that you can identify even the smallest abnormalities in their behavior that may lead to a compromise or indicate a breach in progress. You need to create user profiles that detail their typical activities and behaviors on a day-to-day basis. This will make it easier to flag anything unusual, like a user uncharacteristically handling sensitive data, communicating with unknown people or servers, or any activity that falls outside that user's typical behavior.

As Target learned the hard way, outside service providers provide hackers with an alternative way to infiltrate your network. Consider auditing your service providers to ensure they are using appropriate safeguards. If possible, try to limit their access to only the data and systems needed to fulfill their function. Remote access should be provided when needed but otherwise disabled. Also, service agreements should be reviewed annually to ensure that the indemnification, limitation of liability, and cyber liability insurance provisions are appropriate. These provisions should reflect a balance between the amount of data at risk, the extent of the service provider's access to that data, and the potential costs associated with a data breach. If a service provider has agreed to indemnify your business for data breaches, make sure it has the financial resources to do so, and if not, require cyber liability insurance provisions to cover any shortfall. Be mindful of limitation of liability provisions, which routinely limit liability to the amount of fees collected under the service agreement or within a certain period of time.

Although it may be impossible to eliminate third-party security risks altogether, you can do a better job of containing them through prudent planning, regardless of your company's size or IT budget. With that in mind, here are four important steps a company can take to reduce the risk of data breach when it comes to working with third parties.

- Start with Internal Safeguards and Multiple Layers of Protection. The best way to protect your organization from security threats resulting from work with other vendors is to start from within. Begin by enacting a multi-layered defense strategy that covers your entire enterprise, all endpoints, mobile devices, applications, and data. Those layers should include encryption, and two- or even three-factor authentication for all network and data access requests from third parties. In the case of security, more is generally better, as in more controls and protocols. Of course, the extra layers of security won't function very well unless your IT department is fanatically detailed about doing software updates and patch management in a timely fashion across the network. Also establish a comprehensive data security policy for your employees to follow and never stop educating them about best practices. Take steps to make sure they comply by implementing data classification, access rights and limitations, auditing and more. Above all, counsel them against releasing any security credentials to unauthorized parties. Research shows that credentials are the top threat vector for third-party hacks.
- Make Prevention Essential for Avoiding Vendor-related Threats. Don't pass up opportunities to educate your company, including its Board, CEO, CFO, CMO, and others in command, that the threat is real and prevention is the best policy. Many top executives don't want to throw time, money, and resources at security because they don't see as urgent. But when a breach happens, they'll do anything to put an end to it. Often the organization simply can't recoup some of its losses. Much more money is frequently spent on fixing breaches than on putting preventative practices in place. You also need to educate your vendors about this.
- Perform a Third-Party Vendor Assessment. The biggest third-party hacks in recent years have been the result of organizations giving their business partners access to sensitive information and systems, access to the network, responsibility for managing systems, and responsibility to host data and applications. In reality, your most trusted business partners can pose a security threat if they don't have best practices in place. Some third-party

vendors only need access to your network, while others need access to specific data. Your third-party vendor assessment should start by focusing on access. It should lead to a "least privilege" policy covering who can access your data and network, and specifically what they can access. Regularly review the use of credentials with your third parties and understand who is using them within the partner organization. And limit temporary access, as it potentially opens the door to increased vulnerability. When you engage the services of a third-party vendor, no matter how much you trust them or how long you've worked with them, it is essential to continuously assess the vendor's security standards and best practices to determine if they meet those of your organization. Have them take part in thorough information security assessments at regular intervals, and ensure that all contracts contain clauses detailing their obligations for their own employee background checks as well as for engaging in employee data security training and robust security controls. Also require them to perform up-to-date patching and vulnerability protection of their e-mail and web activities. And make sure you put an auditing or verification program in place to confirm that their contractual obligations are being followed to the letter.
- Create a Service-Level Agreement (SLA) with Your Third-party Vendors. This SLA should mandate that third-party vendors comply with your company's security policies and that your company has the right to audit compliance. Key elements of an SLA should cover information security and privacy, network and data access, disclosure and breach reporting requirements and auditing and verification of compliance. It should also have a threat and risk analysis. Your vendors should also be required to follow NIST guidelines as well as SANS Critical Security Controls.

The risk of data breaches caused by third-party vendors is just far too great to ignore today. While the list above is only a starting point, the important thing is to get started. You have everything to lose if you don't take the security vulnerabilities caused by your vendor relationships seriously. And you have much to gain if you begin planning now.

HIRING EMPLOYEES

Conduct a comprehensive background check on prospective employees. Check references, credit reports, schools attended, licenses, civil judgments, citizenship, criminal records, and personality traits. Unless your business has sufficient in-house expertise and resources for this, you should contract with a knowledgeable and reputable Consumer Reporting Agency (CRA) that is familiar with and will comply with the federal Fair Credit Reporting Act (FCRA), California Investigative Consumer Reporting Agencies Act (UCRAA), Consumer Credit Reporting Agencies Act (CCRAA), and other laws enacted to protect consumers and job applicants. Here a consumer report is defined as any report by a third-party agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. For checks on foreigners, look for a CRA with a presence in the candidate's country of citizenship. And test the CRA by giving it an "applicant" whose background is known so it's the thoroughness and accuracy of its report can be assessed. You should also consult with legal counsel to ensure compliance with federal, state, and local laws. And with so many foreigners being employed, it is also necessary to comply with the laws governing a candidate's country of citizenship. Background checks are heavily regulated and even unintentional mistakes can lead to liability exposure. Care must be taken to achieve compliance with all relevant laws any time an employer starts to investigate the background of a job applicant. Here are some tips to avoid legal liability.

- Don't randomly require background checks. Inconsistency in their use invites claims of discrimination.
- Get the applicant's written consent for the background check in a stand-alone document that clearly states the intent of each report.
- Make sure you use the correct forms.
- Don't assume you can search public records and avoid liability.
- Obtain reports from trusted sources. Extra care should be exercised when gathering information from unknown or unverifiable online repositories.
- Don't ask applicants to self-identify criminal history. More and more jurisdictions are banning early requests for criminal background. In some jurisdictions, including a number of larger cities, employers cannot even ask about arrest history except in limited circumstances. The requirements also vary by type of employer.
- Don't seek protected data, such as medical data, genetic information, or family status. If it is impermissible to ask for such information in an interview, it is likely impermissible for a CRA to obtain.

- Don't seek data that is too old. Consumer reports should not extend past the last 10 years. Any other information more than seven years old except criminal convictions is also usually off limits.
- Keep all background check reports and other documents. There are special rules for disposing of a consumer report.
- Review each report carefully to determine if there's a job-related basis to disqualify an applicant.
- Don't rush through the process or cut corners.

A criminal record check should include arrests, convictions, and outstanding warrants. In considering this information in making employment decisions, follow the U.S. Equal Employment Opportunity Commission (EEOC) Enforcement Guidance No. 915.002 dated 4/25/2012 regarding the prohibition of discrimination under Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e *et seq*. Best practices for employers include the following:

- Eliminate policies or practices that exclude people from employment based on any criminal record.
- Train managers and hiring officials in the EEOC Enforcement Guidance.
- Develop a policy and narrowly-tailored procedures for screening applicants and employees for criminal conduct.
- Identify essential job requirements and the actual circumstances under which the jobs are performed.
- Determine the specific offenses that may demonstrate unfitness for performing such jobs.
- Identify the criminal offenses based on all available evidence.
- Determine the duration of exclusions for criminal conduct based on all available evidence.
- Include procedures for individualized assessments.

Check the applicant's references. This can be very useful when done right because other checks may not reveal any potential problems in the applicant's background. Then because applicants tend to name people who they believe will give you favorable information about them, you should ask each reference to give you the name of someone else who has worked with the applicant. These secondary references will likely give you more objective information about the applicant. A good hiring policy would be to check three references named by the applicant and also three secondary references. Also, if you have anyone in your organization who has worked with the applicant, you should have an off-the-record conversation with them about the applicant.

Test applicants for personality traits as well as job skills. Look for those who can work well with others, show compassion to and for others, respond well to criticism, and communicate frustrations effectively. Applicants that exhibit the following traits are worrisome:

- An exaggerated view of their abilities, achievements, and potential value to an organization
- Intolerant of criticism
- Minimizes the significance of the work of others
- Need for attention and approval
- Excessively emotional
- Overly moralistic
- Strong beliefs on how things should be done
- Unable to compromise, things are black or white and never gray, has the correct problem solution
- Antisocial
- Dishonest in background details and capabilities
- Many job changes
- Lawsuits with prior employers
- Never had difficulties is past relationships

Interview prospective employees. Seek to hire individual who are team-oriented, can respond well to criticism, and can deal well with conflicts, i.e., ones unlikely to become insider threats. Note that California employers are now prohibited from demanding usernames, passwords, and information related to social media accounts from job applicants and employees. The law also bans employers from firing or disciplining employees who refuse to divulge their social media information. This includes videos, photographs, blogs, podcasts, text messages, e-mail, online accounts, and website profiles. However, this prohibition does not apply to information used to access employer-issued electronic devices and is not intended to infringe on the existing rights and obligations of employers to investigate employee workplace misconduct or employee violations of other laws or regulations.

PERSONNEL POLICIES AND EMPLOYEE TRAINING

Employees, including contractors, can do a great deal of damage to a business by ignorance of security policies, negligence in protecting business secrets, deliberate acts of sabotage, embezzlement, and the public release of sensitive information. The following measures will help prevent this.

- Require vendors, suppliers, and other contractors to use similar standards in hiring their employees. Include language in all contracts that makes contractors liable for actions of their employees.
- Treat all employees fairly and make sure none are teased by their peers or supervisors because of their ethnicity, speech, financial situation, social skills, or other traits.
- Monitor activities of employees who handle sensitive or confidential data. Many computer crime schemes require regular, periodic manipulation to avoid detection. Watch for employees who work abnormally long hours, weekends, or holidays, refuse to take time off, or exhibit a sudden withdrawal in group activity. The latter represents dissatisfaction with the business, a common trait of people who are likely to engage in insider security breaches. Also watch for employees who collect material not necessary to their jobs, such as data printouts, software manuals, etc. Unreported foreign trips are also red flags. The biggest security threats come from employees, not foreign hackers.
- Conduct periodic background checks on existing employees and look for unexplained financial gains.
- Train your employees in your basic computer usage and security policies. Also cover penalties for not following your policies. And have employees sign a statement that they understand and will follow your policies.
- Train your employees about security concerns and procedures for handling e-mails, clicking on links to websites, responding to popup windows, and installing USB drives. For example, they should not open e-mail from an unknown sender, open unexpected e-mail attachments, click on any links in e-mail messages even if they look real, respond to popup windows, or install personal USB drives. As for USB drives, you should supply your employees with ones that have built-in encryption.
- Train your employees to be aware of what others, even their supervisors, are doing and to report any suspicious behavior that threatens your cybersecurity.
- Warn your employees about phishing e-mails that appear to come from company executives and request sensitive personal and company information. In the spring of 2016 the IRS investigated several cases in which people were tricked into sharing SSNs with what turned out to be cybercriminals. And on March 1 it published IR-2016-34 to alert payroll and human resources professionals of phishing schemes involving W-2 forms that contain Social Security Numbers (SSNs) and other personally identifiable information. Employees should check out any requests for such information before responding, even if it appears to come from their CEO.
- Develop a culture that actively embraces whistleblowers. Motivate employees to report cybersecurity problems within the business. Research shows that most whistleblowers are not disgruntled employees acting out of greed or spite, but good workers or managers honestly trying to get problems fixed before they will harm to the business. They go outside because they worry that no one is listening inside or worse, that management will "shoot the messengers" and retaliate against them. Thus, businesses need to move quickly to fix reported problems.
- Conduct periodic re-training because people forget things. Use pamphlets, posters, newsletters, videos, etc.
- Prohibit your employees from using their work computers for online shopping. There is a chance that they might unwittingly land on a fake website with an address similar to that of a legitimate company, e.g., Appple.com instead of Apple.com. This would inadvertently expose your computer network to cyber attacks.
- Spread security training over time. Don't rely on one-time seminars by security professionals. Present information in small pieces.
- Make security messages visible. Use videos in training sessions. Put up posters at fax machines, shred bins, coffee rooms, and other places where employees gather. Change them at least once a month. Have a security column in the business newsletter.
- Know your employees. Get views from people in various departments. Be alert to key indicators that an employee may become an insider threat. These include the following:
    - Sudden, apparent devotion to work and working late and alone
    - Accessing data not needed or never used in the past

    - Asking about things they are not involved with
    - Excessive use of "I" in writings and speech
    - Frustration with position and failure to get promoted
    - Lifestyle well above salary level
    - Financial debt
    - Strong objections to procedural changes related to financial, inventory or supply matters
    - Drugs and alcohol abuse
    - Moonlighting with materials available at the business
    - Evidence of compulsive gambling, persistent borrowing or bad check writing
- Make employees aware of insider threats and encourage employees to observe and collect information that indicates stress, and report suspicious behavior. The goal should be to catch an employee in the early stages of stress so they can be helped and prevented from harming themselves or the business.
- Develop protocols that will prevent a departing employee from stealing anything or later harming the business. Remind the employee of the agreements regarding confidentiality, non-disclosure of business information or data, and non-competition that were signed on employment.

MALWARE PROTECTION

Malware, which is short for malicious software, is computer code that's designed to disrupt computer operations, monitor and control online activity, or steal personal information. It includes the following:

- ***Viruses*** are programs that replicate themselves by infecting other programs. They often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing personal information, corrupting data, displaying political or humorous messages, spamming their contacts, or logging their keystrokes.
- ***Worms*** are standalone programs that replicate themselves in order to spread to other computers. Often, they use a computer network for this, relying on security failures on the target computer to access it. Unlike a computer virus, a worm does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- ***Trojans*** are non-self-replicating programs containing malicious code that, when executed, carry out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. Trojans often employ a form of social engineering, presenting themselves as useful or interesting in order to persuade victims to install them on their computers.
- ***Scareware*** is a type of malware that is designed to trick victims into purchasing and downloading useless and potentially dangerous software. It usually appears as a pop-up that resembles Windows system messages and says that a large number of problems have been found on your computer and prompts you to buy software to fix the problems.
- ***Ransomware*** is a type of malware that restricts access to the infected computer system and demands a ransom paid to its creators to have the restriction removed.
- ***Spyware*** is software that gathers information about you, your computer, and your use of the Internet without your knowledge. It may also send that information to another entity or assert control over your computer.
- ***Adware*** is software that displays unwanted advertisements.

The following measures can help protect your computers from viruses, spyware, and other types of malware:

- Keep your computer up to date with the latest operating systems, applications, anti-virus (anti-malware) software and firewalls. The latter control incoming and outgoing network traffic based on an applied rule set. They establish a barrier between a trusted, secure internal network and the Internet or another network that is assumed not to be secure and trusted. Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information. This also applies to multi-function printers, fax machines, and copiers that can be accessed using a web browser.
- Also install real-time e-mail and web security along with solutions that prevent data theft and loss of confidential information. Traditional anti-virus products don't provide this protection.
- Don't open any e-mail from an unknown sender. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an

attachment to get infected. Another way to prevent this kind of attack is to deactivate the display of HTML e-mails and display e-mails in pure-text format only.
- Don't buy or download free anti-virus software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected malicious software.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the advertisement. To be safe on a PC, hold down the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full anti-virus scan.
- Don't respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 11, which is designed to prevent phishing attacks. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.
- Don't install files or programs from CDs or flash drives before checking them for viruses.
- Scan demo disks from vendors, shareware, or freeware sources for viruses.
- Avoid use of electronic bulletin boards.
- Don't download files from unknown sources.
- Don't allow any website to install software on your computers.
- Scan downloaded files for viruses. Avoid downloading executable files.
- Obtain copies of your anti-virus software for your employees' home computers if they do some business work at home. Also ensure that your employees' home computers are protected by hardware and software firewalls between their system(s) and the Internet.
- Approach cybersecurity from the perspective of a potential hacker when deploying or developing new solutions and applications. Avoid reliance on assumptions by employees who have no intention of hacking into the system.

PROTECTING BANK ACCOUNTS

- Set up dual controls so that each transaction requires the approval of two people.
- Establish a daily limit on how much money can be transferred out of your account.
- Require all transfers be prescheduled by phone or confirmed by a phone call or text message.
- Require that all new payees be verified.
- Check bank balances and scheduled payments at the end of every workday rather than at the beginning of the day. Contact the bank immediately if anything is amiss. Timely action can halt the completion of a fraudulent transaction because transfers usually aren't made until the next morning.
- Inquire about your bank's defenses against cyberattacks and review the terms of your banking agreement with regard to responsibilities for fraud losses. Shop around for banks that provide better protections.
- Conduct online business only with a secure browser connection, which is usually indicated by a small lock in the lower right corner of your web browser window. Erase your browser cache, temporary Internet files, cookies, and history after all online sessions. This will prevent this information from being stolen if your system is compromised.
- If your bank does not offer TFA for your account, move it to another bank.

In November 2014 some cybersecurity researchers spotted a strain of malware designed to eavesdrop on business computers in order to steal personal information such as usernames and passwords. Its ultimate aim was to break into bank accounts and siphon off cash. The virus, called Dridex, is spread through infected e-mails sent by its developers to targets. The e-mails typically contain an infected Microsoft Office file and attempt to trick the user into opening the attachment. If the user opens the document, a macro embedded in it surreptitiously triggers a download of the Dridex banking malware, enabling it to first steal banking credentials and then attempt to generate fraudulent financial transactions. In August 2015 the botnet that controlled much of the Dridex network was seized by the U.S. authorities and one of the co-conspirators arrested. The spread of the malware stopped immediately. However, the software itself still exists, and researchers warn that it be used by other criminal groups with their own botnets. The measures listed above along with those for protecting against most other malware attacks should protect a user's computers against a Dridex-type attack. Users should have an up-to-date antivirus program running on their computer that can intercept the infected attachments before they are seen. Users should also be careful of opening attachments sent from unrecognized e-mail addresses.

USING SOCIAL MEDIA

While the use of social media can stimulate innovation, create brand recognition, generate revenue, and improve customer satisfaction, it has inherent risks that can negatively impact business security. Thus businesses need to develop a social media strategy and a plan to address the risks of business and employee use. These risks include the following:

- Data leakage or theft
- Data system downtime to clean malware
- Exposure of customer confidential information
- Spear phishing attacks on customers and employees
- Adverse legal actions
- Privacy violations
- Brand and reputation damage
- Loss of competitive advantage
- Infection of mobile devices
- Productivity loss from excessive employee use
- Circumvention of business controls

Some risk mitigation techniques for business and employee use of social media are listed below. For details on risks and mitigation techniques see the emerging technology white paper entitled *Social Media: Business Benefits and Security, Governance and Assurance Perspectives* published by the Information Systems Audit and Control Association (ISACA).

- Conduct awareness training to inform employees of the risks in using social media.
- Ensure that anti-virus controls are updated daily.
- Use content filtering to restrict or limit access to social media sites.
- Provide employees with clear guidelines regarding what information about the business can and cannot be posted on their personal sites.
- Limit use of social media on business computers and devices.
- Scan the Internet for unauthorized or fraudulent use of the business name or brand, or hire a brand-protection firm to do this.
- Require strong passwords for site access by its managers.
- Give customers periodic information updates to maintain awareness of potential fraud.
- Establish policies for the use of mobile devices to access social media.
- Install appropriate controls on mobile devices.
- Obtain access to employees' personal sites and monitor them for security breaches.

CYBERSECURITY PLANNING

The following resources are available to help businesses in cybersecurity planning.

Federal Communications Commission (FCC)

One way small businesses can improve their cybersecurity is to use the Small Biz Cyber Planner that was created by the Federal Communications Commission (FCC) in collaboration with public and private sector partners, including the Department of Homeland Security, the National Cyber Security Alliance, and the Chamber of Commerce. It can be created and generated at **www.fcc.gov/cyberplanner**.

This planning guide, Small Biz Cyber Planner 2.0, is designed for businesses that lack the resources to hire a dedicated staff to protect themselves and their customers from cyber threats. Even a business with one computer or one credit card terminal can benefit from this tool. The planner deals with the following topics.

- Privacy and Data Security. Nothing is more important than the security of your data. How you handle and protect it is central to the security of your business and the privacy expectations of all the people involved.
- Scams and Fraud. Telecommunication technology offers cyber criminals many ways to victimize your business, scam your customers, and hurt your reputation. You need to be aware of the most common online scams.
- Network Security. For this you need to: (1) identify all devices and connections on the network, (2) set boundaries between your systems and others, and (3) enforce controls to ensure that unauthorized access, misuse, or denial-of-service attacks can be thwarted or rapidly contained, and that your systems can recover from these threats.
- Website Security. Web servers that host the data and other content available to the public on the Internet are the most targeted components of a business' network. Cyber criminals are constantly looking for websites to attack. Thus it is essential that your servers and the network infrastructure that supports them be secure because a breach can cause loss of revenues and customer trust, and legal liability.
- E-mail. E-mail has become vital for everyday operations. It must be secure to ensure the privacy of its users and to protect customer and business information.
- Mobile Devices. Mobile devices such as smartphones, tablets and Wi-Fi enabled laptops, if not secure, can expose and compromise all your business networks.
- Employees. Businesses must establish formal recruitment and employment processes to control and preserve the quality of their employees. Otherwise they risk workplace violence, theft, embezzlement, lawsuits for discrimination in hiring, and other workplace problems.
- Facility Security. Protecting those who work in and visit your business should be one of your top priorities.
- Operational Security. These measures are designed to deny hackers access to any information about your operations and plans.
- Payment Cards. These measures prevent fraud, keep customer information safe, and enable you to meet obligations to your bank or payment services processor.
- Incident Response and Reporting. Even well-implemented security measures cannot prevent all breaches, so be sure to have procedures in place to respond to breaches if they occur.
- Policy Development and Management. All businesses should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputation, and discouraging inappropriate behavior by employees. These need to be tailored to your business and updated when needed to deal with new threats and problems.

If your business uses more sophisticated networks with dozens of computers, the FCC recommends that you consult a cybersecurity expert on using the cyber planner. Also, the FCC provides no warranties with respect to the guidance provided by this tool and is not responsible for any harm that might occur from using it.

U. S. Department of Health and Human Services

At **www.HealthIT.gov** under Providers and Professionals, Privacy and Security, and Security Risk Assessment (SRA) there is a SRA tool and video, a 10-step privacy and security plan, a *Guide to Privacy and Security of Health Information*, and other information for cybersecurity planning that can be used in any business.

Greater Houston Partnership

At **www.Houston.org/cybersecurity** you can fill out a Cybersecurity Self Assessment Tool to measure your vulnerability to a cyber attack. It will tell you whether you have good security measures in place, whether you should perform a risk-benefit analysis to determine what additional measures to install, and whether you need to invest in more cybersecurity. You should also review the guide entitled *Cybersecurity and Business Vitality*. Although it was prepared for Houston-area businesses, it is applicable anywhere for any business.

U.S. Department of Homeland Security Computer Emergency Readiness Team (US-CERT)

At **www.us-cert.gov/home-and-business** you can keep up to date on a variety of subjects related to cybersecurity. These include the basics of cloud computing, virus safety on social networking sites, understanding denial-of-service attacks, avoiding social engineering and phishing attacks, choosing and protecting passwords, 10 ways to improve the security of a new computer, etc. You can also get current activity, alerts, bulletins, and tips from the National Cyber Awareness System.

CERT Coordination Center

Before US-CERT, the Software Engineering Institute at Carnegie Mellon University ran the CERT Coordination Center. At **www.cert.org/information-for/managers** managers can use the material on this site, which includes podcasts, to keep their employees informed about cybercrime and help them protect your business from malicious attack. The site also provides answers to the following questions: Are your networks secure? Are you doing enough about insider threats? How resilient is your organization? How well are you incorporating security into your products and services? Are you addressing the latest software vulnerabilities? Are you responding effectively to incidents? Do you know how a Computer Security Incident Response Team (CSIRT) can help you?

SANS Institute

At **www.SANS.org/security-resources** you can see the *Top 25 Software Errors* that lead to serious vulnerabilities, the *20 Critical Controls* for effective cyber defense, and 12 templates for various security policies from the SANS Security Policy Resource page. These include policies for computers, desktops, e-mail, Internet use, mobile devices, etc. There is also a short primer for developing policies.

NIST

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013. It directed NIST to work with stakeholders to develop a voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure. NIST released the first version of the framework on February 12, 2014. It was created through collaboration between industry and government and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. This framework and its companion roadmap can be used in any business. It is available on line at **www.nist.gov/cyberframework**.

U. S. Chamber of Commerce

The U.S. Chamber of Commerce has teamed with Bank of America, Microsoft, Splunk, and Visa up to provide businesses with the guide that gives small- and medium-size businesses tools for protecting computers and networks and responding to cyber incidents. The guide, *Internet Security Essentials for Business 2.0*, urges business owners, managers, and employees to adopt fundamental Internet security practices to reduce network weaknesses and make the price of successful hacking increasingly steep. It emphasizes the following points and can be downloaded at **www.uschamber.com/sites/default/files/legacy/issues/defense/files/020956_PDF_web.pdf**.

- All businesses should understand common online risks that may lead them to become victims of cybercrime.
- Perfect online security is unattainable, even for large businesses. But there are inexpensive practices that can be implemented to improve the security of your information, computers, and networks.
- Businesses need to know how and to whom to report cyber incidents and online crime.
- Cybersecurity is a team activity. Taking the actions recommended in this guide will have positive consequences for the security of businesses, communities, and the country. The interconnectedness of computers and networks in cyberspace means that the public and private sectors share responsibility.

Its website at **www.uschamber.com/issue-brief/internet-security-essentials-business-20** provides links to the guide mentioned above and the following Microsoft tools that businesses can use to teach employees how to protect business, customer, and employee information.

- Top Tips for Internet Security at Work, a printable, double-sided card
- Internet Security at Work PowerPoint, a 30-minute slide presentation with speaker's notes.
- Stay Sharp on Internet Safety at Work, information condensed into a 3-minute video.
- Test Your Internet Security IQ, a 10-question quiz to help spread awareness among your employees.
- Internet Security Begins With You, a poster to remind employees of their responsibilities for Internet security

SECURITY FOR MOBILE DEVICES

When it comes to security, most mobile devices are targets waiting to be attacked by cybercriminals. That's the conclusion of GAO-12-757, a September 2012 report to Congress by the U. S. Government Accountability Office. This report, entitled *Better implementation of Controls for Mobile Devices Should Be Encouraged*, can be downloaded from the GAO website at **www.gao.gov/assets/650/648519.pdf**. It lists a number of vulnerabilities and threats and suggests several security controls to combat them.

These controls include the following:

- Enable user authentication. Configure devices to require passwords or PINs to gain access.
- Enable TFA for sensitive business information. It's usually done under Settings or Privacy. TFA makes if far more difficult for cybercriminals to break into online accounts.
- Verify to authenticity of downloaded applications.
- Install anti-virus software to protect against spyware and other types of malware.
- Install a firewall to protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules.
- Implement procedures to receive security software updates promptly.
- Install remotely disabling so that if the device is lost or stolen, it can be locked or its contents erased.
- Encrypt sensitive data.
- Install whitelisting software that permits only known safe applications to execute commands.
- Only install necessary applications.

Cybercriminals are also targeting mobile devices with malware that compromises these devices. The IC3 suggests the following safety tips to protect them.

- When purchasing a smartphone, know the features of the device, including its default settings. Turn off features that are not needed to minimize the attack surface of the device.
- If the phone's operating system has encryption available, use it to protect your personal data in the case of loss or theft.
- With the growth of the application market for mobile devices, look at the reviews of the company that published the application.
- Review and understand the permissions you give when you download applications. Understand their privacy and access setting. Be cautious in downloading applications and be aware of what data they access as a condition of their use. Look for comments other users post before downloading an application.

- Passcode protect your device. This is the first layer of physical security to protect its contents. In conjunction with the passcode, enable the screen lock feature after a few minutes of inactivity.
- Obtain malware protection. Look for applications that specialize in antivirus or file integrity that helps protect your device from rogue applications and malware.
- Be aware of applications that can track your location. They can be used by a criminal to assist a stalker or a burglar.
- Be aware that using jailbreak or rooting to remove certain restrictions imposed by the device manufacturer or cell phone carrier, which allows you nearly unregulated control over what programs can be installed and how the device can be used, often exploits significant security vulnerabilities and increases the attack surface of the device. Any time a user, application, or service runs in "unrestricted" or "system" level within an operational system, any compromise can take full control of the device.
- Don't allow your device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and a legitimate server.
- If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.
- Install all smartphone updates to run applications and firmware. If you neglect this you risk having your device hacked or compromised.
- Avoid clicking on or otherwise downloading software or links from unknown sources.
- Use the same security precautions on your mobile phone as you would on your computer when using the Internet.

Businesses should also develop a mobile-device security policy. The policy would define the rules, principles, and practices for employee use of mobile devices, whether they are issued by the business or owned by an employee. It should cover roles and responsibilities, infrastructure security, device security, and security and risk assessments. By establishing policies that address these areas, agencies can create a framework for applying practices, tools, and training to help support the security of wireless networks. The business should also train its employees in this policy to ensure that mobile devices are configured, operated, and used in a secure and appropriate manner.

Mobile device security is especially important when employees are allowed or even encouraged to use their own mobile devices, known as Bring Your Own Device (BYOD). Businesses need a policy for BYOD use so they can be sure that: (1) business and personal information are kept separate in the device, (2) malware on an employee's device doesn't get into the business network, (3) an outsider can't hack into the employee's device and get into the business network or steal sensitive business information, and (4) all business data can be removed from the device when the employee leaves or if the device is lost or stolen.

Businesses can avoid common weaknesses in smart devices by disabling unnecessary functionality such as cameras, Bluetooth, and Wi-Fi, and keeping these devices up to date and secured just as they would for any other business system. They should also make sure that the default passwords and other settings are changed.

DATA PRIVACY AND SECURITY WHEN TRAVELING WITH MOBILE DEVICES

Corporate espionage is an increasingly serious threat for a business traveler. The perpetrator may be a competitor, opportunist, or foreign intelligence officer. In many countries, domestic corporations collect competitive intelligence with the help and support of their government. To mitigate this risk, critical business data should not be carried in print or on an electronic device unless it is absolutely necessary. If some must be carried, it should be encrypted. And the traveler should keep it on his or her person at all times. Mobile devices should never be unattended. Hotel safes are not adequate protection.

Security is also a concern when using business data in other countries. For example, the U.S. State Department's Bureau of Consulate Affairs advisory for the 2014 Sochi Olympics stated that "Travelers should be aware that Russian Federal law permits the monitoring, retention, and analysis of all data that traverses Russian communication networks, including Internet browsing, e-mail messages, telephone calls, and fax transmissions." Thus, conversations may not be private or secure, and wireless and other communications may be intercepted. Some measures that a traveler should take to protect business data before, during, and after travel are suggested below.

Before Travel

- Minimize data taken on removable media such as CDs, DVDs, and thumb drives.
- Consider using a business-owned cell phone, laptop, and/or tablet that contains only necessary data to limit the loss of data if the device is lost, stolen, or confiscated.
- Back up all data taken and store it in a secure place while you are away.
- Clear your Internet browser's cache, cookies, history and temporary Internet files.
- Update data protection software prior to departure.
- Install full-disk encryption on laptops.
- Use the U.S. State Department website at **www.state.gov** for information on the country of travel and laws regarding bringing mobile devices in and out. For example, Russia has no restrictions on bringing laptop computers into the country for personal use. However, the software may be inspected upon departure. Hardware and software found to contain sensitive or encrypted data may be subject to confiscation. In some countries withholding passwords is a crime.
- Install new strong passwords on all devices, with different ones on each one.
- Configure settings to automatically wipe devices' data after a certain number of password entry failures.
- Check with your business' legal advisor and IT manager for other measures to take.

During Stay

- Do not expect privacy in some countries. Phone calls, electronic transmission, and even hotel rooms may be monitored. Sensitive conversations, transactions, and data transfers should be kept to a minimum until you return.
- Be prepared to turn devices on and off, present all removable media to customs officials, and decrypt data for inspection at international borders.
- Keep social networking communications and business transactions separate on your devices.
- Consider buying local cell phones or local Subscriber Identity Module (SIM) cards. Prepaid local phones limit costs by not working after exceeding a maximum number of minutes. They are cheaper for local calls and have better connectivity. Buying local Pay As You Go (PAYG) SIM cards provide an added level of anonymity that may be good for privacy and security.
- Beware of Wi-Fi and hotspot dangers, as discussed in the next section.
- Do not loan your devices to anyone.
- Do not attach unknown thumb drives. They are notorious for computer infections.
- Report lost or stolen devices as soon as possible to all concerned parties, which might be your business, mobile service provider, etc. Also report the loss to local authorities.

On Return

- Return business-owned borrowed devices.
- Test all devices and removable media for malware, unauthorized access, and other corruption. Do not connect them to a trusted network before testing
- Reformat and rebuild any device found to be compromised. Then restore data from files backed up before your travel.
- Change passwords on all devices taken on travel.

Other safety and security measures for business travel outside the U. S. are contained in a FBI brochure at **www.fbi.gov/about-us/investigate/counterintelligence/business-brochure**.

WI-FI HACKING AND HOTSPOT DANGERS

Use of Wi-Fi in coffee shops, libraries, airports, hotels, universities, and other public places pose major security risks. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information. If the hotspot doesn't require a password, it's not secure. If it asks for a password through your browser simply to grant access, or it asks for a Wired Equivalent Privacy (WEP) password, it's best to treat it as unsecured. You can be more confident that a hotspot is secure only if it asks for the Wi-Fi Protected Access (WPA and WPA2) password. WPA2 is more secure. However, a flaw in a feature added to Wi-Fi called Wi-Fi Protected Setup (WPS) allows WPA and WPA2 security to be bypassed and broken by brute force in many situations.

Also, unsecure laptops and smartphones make it easy for a hacker to intercept information to and from the web, including passwords and credit or debit card numbers. They are also vulnerable to malware infections, and to having their contents stolen or destroyed. A hacked laptop or smartphone can also create a security risk for the user's workplace if it contains a password to the corporate network. Wi-Fi users should take the following steps to reduce these risks:

- Turn the Wi-Fi on your laptop, PDA, and smartphone off when you aren't using the network. Otherwise your Wi-Fi card will broadcast your Service Set Identifier (SSID) looking for all networks it was previously connected to. This enables hackers to figure out the key that unscrambles the network password.
- Use a known service instead of Free Public Wi-Fi or similar risky, unknown signals called ad hoc networks.
- Check the Wi-Fi security policies of your service provider and install the protections they offer to ensure it's a known network and not an "evil twin" hacker site pretending to be the legitimate one.
- Pay attention to warnings that a Secure Sockets Layer (SSL) certificate is not valid. Never accept an invalid certificate on a public wireless network. Log off and look for a trustworthy network. Look for the padlock indicating an SSL connection. Keep your firewall on. And keep your operating system updated.
- Find out if your business offers a Virtual Private Network (VPN) and learn how to use it. Encrypted VPN sessions offer the highest security for public wireless use. Use Hypertext Transfer Protocol Secure (HTTPS) when accessing a website or use a VPN to protect the transmission of sensitive information when using a wireless connection.
- Upgrade your Wi-Fi cards. The older WEP security is easily hacked. The new WPA and WPA2 are much more resistant to attack.
- Secure IEEE 802.11 wireless access points with a WPA2 and Advanced Encryption Standard (AES) encryption to protect sensitive communications.
- If your router has the WPS function, disable it. Methods have been published for doing this for some models. But on others, disabling the WPS in the user interface is not effective and the device remains vulnerable to attack.
- Learn to connect securely. Even the vulnerable WEP offers more privacy and protection than an unsecured public connection. It's not something the average hacker can crack. Make sure your connection is legitimate. Look at your connection page for a name and description. A legitimate wireless network is simply called a "wireless network." It will display an icon of just one connected computer. So called ad hoc or peer-to-peer networks that are used by scammers to steal your personal information scammers are not legitimate. The will be called "computer-to-computer" networks and display an icon of several computers connected together. Never connect to this network. And be sure to set up your computer so it doesn't automatically connect to a network but allows you to choose a connection.
- Only log in or send personal information on website pages that are encrypted. They will have **https://** or **shttp://** in their addresses and a "lock icon" at the top or bottom of your browser window. You can click on this icon to display information about the website and help you verify that it's not fraudulent.
- Use a different password for each account.
- When you've finished using an account, log out. Don't stay signed in.
- Pay attention to warnings from your browser if you try to visit a fraudulent website or download a malicious program.
- Remove all passwords and browsing history after using a shared computer.
- Disable file-sharing on your laptop.
- Don't send any sensitive personal or business information while in a hotspot unless you absolutely have to.
- Put a unique, strong password on your wireless network. Avoid using easily remembered numbers or available information like mother's maiden name or date of birth. Passwords should have more than eight characters, with at least one capital letter, one lowercase letter, one number, and one symbol. Use of non-dictionary words or easily-remembered phrases is recommended, e.g. Johnhave3dawgs! Hackers can run a program that goes through the entire dictionary very quickly and crack any password which can be found in it. They can also use

grammar rules to crack long passwords, especially those with pronouns. So use bad grammar and nouns. For maximum security you should use passwords that are at least 12 characters long, completely random, and have at least one capital letter, one lowercase letter, one number, and one symbol. You can test your passwords and get advice on creating strong ones at **www.microsoft.com/protect/yourself/password/checker.mspx**.
- Be aware of the existence of malware that enables a mobile phone to be used as an open microphone with or without the owner's knowledge.

Your IT manager should also do the following to protect corporate data from hotspot dangers:

- Establish and enforce strong authentication policies for devices trying to access corporate networks.
- Require employees to use a corporate VPN and encryption when making connections and exchanging data. Better still, set up computers so that devices automatically connect to the VPN and encrypt data after making sure that the computer or device hasn't been lost or stolen.
- Make sure all devices and software applications are configured properly and have the latest patches.
- Ensure that corporate security policies prevent employees from transferring sensitive data to mobile devices or unauthorized computers.
- Provide employees with broadcast air cards that require a service plan so they don't have to use public hotspots for wireless connections.

SAFER USE OF THE INTERNET

Many U.S. Government agencies are involved in promoting safe cyber practices. The main ones are the Department of Homeland Security (DHS) and the Federal Trade Commission (FTC). Four of their programs are described below.

National Cyber Awareness System

Persons with specific concerns about cybersecurity should visit the US-CERT website at **www.us-cert.gov**. US-CERT leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. Its National Cyber Awareness System offers a variety of information for users with varied technical expertise. Those with more technical interest can read or subscribe to the Alerts, Current Activity Updates, or Bulletins. Those looking for more general-interest pieces can read the Tips. Current Activity Updates provide timely information on security risks to help you better protect your systems from malware campaigns and mitigate new software vulnerabilities. It is updated frequently and typically contains less detail than Alerts, which warn about vulnerabilities, incidents, and other security issues that pose major risks. Bulletins provide weekly summaries of new vulnerabilities with patch information provided when available. Tips provide advice about common security issues for home and business users. They deal with general security, attacks and threats, e-mail and communication, mobile devices, privacy, safe browsing, software, and applications.

You can take the following are steps to protect your privacy and personal information.

- Do business with credible companies. Before supplying any personal information online, consider the answers to the following questions: Do you trust the business? Is it an established organization with a credible reputation? Does the information on the site suggest that there is a concern for the privacy of user information? Is there legitimate contact information provided?
- Limit cookies to make sure that other sites are not collecting personal information about you without your knowledge. Choose to allow cookies only for the website you are visiting, and block or limit cookies from a third-party. Make sure that cookies are disabled if you are using a public computer.
- Don't use your primary e-mail address in online submissions. Submitting your email address could result in spam. Consider opening an additional e-mail account for use online if you don't want your primary e-mail account flooded with unwanted messages. Make sure to log onto the account on a regular basis in case the vendor sends information about changes to policies.

- Avoid submitting credit card information online. Some companies offer a phone number you can use to provide your credit card information. Although this does not guarantee that the information will not be compromised, it eliminates the possibility that attackers will be able to hijack it during the submission process.
- Devote one credit card to online purchases. Consider opening a separate credit card account for use online to minimize the potential damage of an attacker gaining access to your credit card information. Keep a minimum credit line on the account to limit the amount of charges an attacker can accumulate.
- Avoid using debit cards for online purchases. Credit cards usually offer some protection against identity theft and may limit the monetary amount you will be responsible for paying. Debit cards don't offer that protection. Because the charges are immediately deducted from your account, an attacker who obtains your account information may empty your bank account before you even realize it.
- Take advantage of options to limit exposure of personal information. Default options on certain websites may be chosen for convenience, not for security. For example, avoid allowing a website to remember your password. If your password is stored, your profile and any account information you have provided on that site is readily available if an attacker gains access to your computer. Also evaluate your settings on websites used for social networking. The nature of those sites is to share information, but you can restrict access to certain information so that you limit who can see what.

Stop.Think.Connect

In 2009 President Obama recognized the need to increase education and dialogue about cybersecurity and issued the Cyberspace Policy Review, which became the blueprint for cybersecurity in the future. In this review the DHS was asked to create an ongoing cybersecurity awareness campaign. It was called Stop.Think.Connect and was launched in October 2010. It provides tips and resources for cybersecurity on its website at **www.dhs.gov/stopthinkconnect**. They include the following.

Before you use the Internet take time to understand the risks and learn how to spot potential problems.

- Stop hackers from accessing your accounts, use strong passwords that are at least 12 characters long, completely random, and have at least one capital letter, one lowercase letter, one number, and one symbol.
- Stop posting and sharing too much, keep your personal information personal.
- Stop doing something if it doesn't feel right, trust your gut.
- Stop questionable online behavior, only do and say things online that you would do in real life.

Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact the safety of yourself and your family.

- Think about the information you want to share before you share it.
- Think how your online actions can affect your offline life.
- Think before you act, don't automatically click on links.
- Think about why you are sharing information online. Is it going to be safe?
- Think about why you're going to a website. Did you get it from someone you trust?
- Think **a**bout who you're talking to online. Do you *really* know who they are?

Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

- Connect over secure networks.
- Connect with people you know and trust.
- Connect with care and be on the lookout for potential threats.
- Connect safely and show your friends and family how to behave online.
- Connect with websites you trust.

Keep a clean machine:

- Have the latest security software, web browser, and operating system.
- Use programs that automatically connect and update your security software.
- Protect all devices that connect to the Internet from all malware.
- Set up local administrator accounts on your computing devices so only an administrator (you) can download programs and applications. Then only download from a trusted source. If you have any questions about the legitimacy of a site, don't download from it.
- Use your security software to scan all USBs and other external devices before attaching them to your computer.

Protect your personal information:

- Secure your accounts with strong passwords.
- Keep a list of your passwords stored in a safe place away from your computer.
- Use privacy and security settings to limit who you share information with.

Connect with care:

- Delete any suspicious e-mail, tweets, posts, and online advertising. When in doubt, throw it out.
- Limit the business you conduct from Wi-Fi hotspots and adjust your security settings to limit who can access your computer.
- Secure your home wireless network. The minimum level of encryption is WPA2. Replace your router if it can't run WPA2. Protect your router with a strong password. The following website has good information on wireless routers: **www.onguardonline.gov/articles/0013-securing-your-wireless-network**.
- Use only secure websites when banking and shopping, i.e., ones with **https://** or **shttp://** in their addresses.

Be web wise:

- Keep pace with new ways to stay safe online by checking trusted website for the latest information.
- Think before you act when you are implored to act immediately, offered something that sounds too good to be true, or asked for personal information.
- Back up your valuable information by making an electronic copy and storing it in a safe place.

Be a good online citizen:

- Practice good online safety habits.
- Post about others as you would have them post about you.
- Report all types of cybercrime to you local law enforcement agency and other appropriate authorities.

OnGuardOnline.gov

The FTC manages this website in partnership with the DHS in its Stop.Think.Connect campaign, and many other federal agencies. Its website, **www.OnGuardOnline.gov**, provides practical tips from the federal government to help you guard against internet fraud, avoid scams, secure your computers, protect your privacy, protect your kids online, be smart online, etc.

Stop.Think.Click

This effort defines seven practices for safer computing and provides tips on preventing identity theft, safe use of social networking sites, online shopping, Internet auctions, avoiding scams, and wireless security. It also provides a glossary of terms. The seven practices are:

1. Protecting your personal information
2. Knowing who you're dealing with
3. Using anti-virus software as well as a firewall

4. Setting up your operating system and web browser software properly, and updating them regularly
5. Protecting your passwords
6. Backing up your important files
7. Learning who to contact if something goes wrong online.

Go to **http://csrc.nist.gov/groups/SMA/fasp/documents/security_ate/stopthinkclick.pdf** for information about these practices and tips.

PREVENTING AND DEALING WITH DATA BREACHES

The number of U.S. data breaches hit a record high of 783 in 2014 according to an Identity Theft Resource Center report sponsored by IDT911. This report is available online at **www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html**. This represents a 27.5 percent over the number of breaches reported in 2013. To help California business deal with this growing problem the Attorney General published a paper entitled *Cybersecurity in the Golden State* in February 2014. It is available online at **https://oag.ca.gov/cybersecurity**. It suggests the following 10 measures to reduce the chances of becoming a victim of cybercrime: (1) Assume you're a target, (2) Lead by example, (3) Map and analyze your data, (4) Encrypt your data, (5) Bank securely, (6) Defend yourself, (7) Educate employees, (8) Be password wise, (9) Operate securely, and (10) Plan for the worst. It also provides basic guidance for preparing an effective cybersecurity incident response plan.

Another paper that provides information to help protect personal information in your business and prevent data breaches was published by the FTC in November 2011. It is entitled *Protecting Personal Information: A Guide for Business* and can be found online at **www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf**. It suggests the following five key principles: (1) Take stock, (2) Scale down, (3) Lock it, (4) Pitch it, and (5) Plan ahead. You should do the following for each.

1. Take stock: Know what personal information you have in your files and in your computers.

- Inventory all file-storage and electronic equipment. Know where your business stores sensitive data.
- Talk to your employees and outside service providers to determine who sends you personal information and how it is sent.
- Consider all the personal information you collect from customers, and how you collect it.
- Review where you keep the information you collect, and who has access to it.

2. Scale down: Keep only what you need for your business.

- Use SSNs only for required and lawful purposes. Don't use them for employee or customer identification.
- Keep customer credit or debit card information only if you have a business need for it. Don't keep any information you don't need.
- Change the default settings on your software that reads customer's credit or debit cards.
- Review the credit application forms and fill-in-the-blank web screens you use to collect data from potential customers, and eliminate requests for any you don't need.
- Use no more that the last five digits of credit or debit card numbers on electronically printed receipts that you give to your customers. And don't use the card's expiration date.
- Develop a policy for retaining written records that is consistent with your business needs and the law.

3. Lock it: Protect the information that you keep and transmit.

- Keep documents and other materials containing personal information in locked rooms or file cabinets.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Create a security policy for your employees when using laptops in and out of your office. (See prior section on Special Measures for Laptops.)
- Control access to your building.

- Encrypt sensitive information you send over public networks or use a secure file transfer service. Don't send personal information by e-mail.
- Run up-to-date anti-virus programs on all your computers. Use a firewall to protect your computers and network. (See prior section on Malware Protection.)
- Require employees to use strong passwords.
- Set access controls so employees only have access to information they need for their jobs. (See prior section on Procedural and Operational Protective Measures.)

4. Pitch it: Properly dispose of what you no longer need.

- Create and implement secure information disposal practices for employees in your office and for those who travel or work at home.
- Train your staff to separate sensitive and other paper records. Dispose of the former by shredding, burning, or pulverizing them. Use cross-cut shredders. The latter can be put in the trash.
- Make shredders available throughout your office, especially next to the copiers.
- Remove and destroy the hard disk of any computer or copier headed for the junkyard. Or wipe them securely.
- Remove and securely wipe hard drives of rented copiers before returning them. Or clear the memory and change the pass codes.
- Destroy CDs, floppies, USB drives, and other data storage devices, or securely wipe them before disposal.
- Test how thoroughly factory resets and remote wipes destroy data on any smartphones your employees use in the business, and only permit them to use phones on which the data can be completely destroyed when the device is retired. If there is any doubt about this, use a hammer on the phone to make sure it does not get into the secondary market.

5. Plan ahead: Create an incident response plan for dealing with security breaches.

- Organize a response team and designate a team leader to manage the activities.
- Draft a plan for dealing with various kinds of breaches, including hacking, lost laptop, etc. The plan should be a flexible playbook that evolves over time had helps guide your responses.
- Review the plan periodically. Are there ways to improve it? Does it provide enough detail? Should any procedures be changed or updated? Does it consider changes in your business? Is personnel contact information up to date?
- Conduct annual tabletop exercises to practice responses in a low-stress, informal setting. These can help identify gaps in your incident response plan and suggest ways you can be better prepared for breaches.
- Investigate breaches immediately and take steps to eliminate existing vulnerabilities or threats to personal information.
- Perform a risk assessment. If you do not know what sensitive personal information and business data you have, where it resides, and who has access to it, you cannot implement appropriate safeguards to protect it. When facing a potential data breach, the inability to provide an accurate network diagram and describe the business' sensitive data flow will complicate the forensic investigation. Risk assessments can help address these issues and should be performed on a regular basis to account for new vulnerabilities, changes to the business' structure or operations, and the ability of existing security controls to detect and defend against likely cyberattacks.
- Disconnect a compromised computer from the Internet.
- Post information about the breach on your website and include the phone number and e-mail address of your customer service staff.
- Create a list of who to notify inside and outside of your business in the event of a breach. The latter include the appropriate law enforcement agencies, the persons whose information has been compromised, your customers and other businesses that may be affected, and the media.
- Draft notification letters and other written communications. Consult your attorney for the latest state and federal notification requirements.
- Consider what outside assistance is needed, e.g., in forensics, media relations, etc.

In June 2015 the FTC published a paper entitled *Start with Security: A Guide for Business*. It contains ten lessons learned from the more than 50 law-enforcement actions the FTC has announced for keeping sensitive data secure.

They touch on vulnerabilities that could affect your business, and provide practical guidance on how to reduce the risks they pose. They are available online at **www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business?utm_source=govdelivery**. Here's an outline of these lessons.

1. Start with Security. Don't collect personal information you don't need. Hold on to information only as long as you have a legitimate business need. Don't use personal information when it's not necessary.
2. Control access to data sensibly. Restrict access to sensitive data. Limit administrative access.
3. Require secure passwords and authentication. Insist on complex and unique passwords. Store passwords securely. Guard against brute force attacks. Protect against authentication bypass.
4. Store sensitive personal information securely and protect it during transmission. Keep sensitive information secure throughout its lifecycle. Use industry-tested and accepted methods. Ensure proper configuration.
5. Segment your network and monitor who's trying to get in and out. Segment your network. Monitor activity on your network.
6. Secure remote access to your network. Ensure endpoint security. Put sensible access limits in place.
7. Apply sound security practices with developing new products. Train your engineers in secure coding. Follow platform guidelines for security. Verify that privacy and security features work. Test for common vulnerabilities.
8. Make sure your service providers implement reasonable security measures. Put it in writing. Verify compliance.
9. Put procedures in place to keep your security current and address vulnerabilities that may arise. Update and patch third-party software. Heed credible security warnings and move quickly to fix them.
10. Secure paper, physical media, and devices. Store sensitive files securely. Protect devices that process personal information. Keep safety standards in place when data is en route. Dispose of sensitive data securely.

Regarding notification, that California Civil Code Sec. 1798.82 requires any person or business that conducts business in California and that owns or licenses computerized data that includes personal information to notify persons whose personal information has been compromised and specify the information involved. This notice requirement is triggered if the breach involves an individual's first name or first initial and last name in combination with one or more of the following data elements when either the name or the data elements are not encrypted: SSN; driver license number or California identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; health insurance information; or a user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account. The letter of notice should also recommend measures to take to deal with the breach, warn of attempts to obtain personal information by e-mail, and suggest that any such attempts be reported to your customer service staff immediately.

In addition to notifying persons whose personal information has been compromised, businesses should do the following to keep their customers informed about what they are doing to fix the problem and regain their trust.

- As with any crisis, the first thing your customers want to know is that you're aware of the situation and that you're on top of it. A simple statement that comes as soon as you are aware of the breach goes a long way towards muting initial panic. This initial response doesn't need to go into a lot of detail about how many were affected, what was hacked, and how it happened. Chances are you won't know that yet so a simple message that doesn't go beyond what you know is best.
- Make sure you have a spokesperson who can communicate effectively about the breach and what you are doing about it. That person does not always have to grant interviews to the press but can make statements on social media instead.
- Share verifiable facts quickly as they come in. Your goal is to get control of the situation and make yourself the most up-to-date source of accurate information. If you don't, others will put forth their own theories about the reason and extent of the attack.
- Keep the public and stakeholders in the loop as you move forward in your investigation using traditional, online, and even paid media. Your website should be THE best source for information. Show it there in three places: (1) the home page, (2) the number one item in your news section, and (3) on a dedicated page that deals with the breach.
- Offer your customers free credit monitoring as the first step to rebuilding their trust.
- Tell your customers what you're doing to protect them from breaches in the future.
- Make an apology that acknowledges the breach and demonstrates concern and compassion for its victims.

- After your IT staff has done its investigation and fixed the problems, assure your customers that cybersecurity is an ongoing concern and that you are working to prevent any breaches in the future.

Regarding outside assistance, businesses should take precautions during their breach investigation to help shield the information provided by outside technical experts from discovery by opposing counsel in the event of litigation. This is necessary because the attorney-client privilege and the work-product doctrine are not absolute. In the class-action litigation arising from Target's massive 2013 data breach, Target asserted the attorney-client privilege and work-product doctrine in defense of the plaintiff's discovery request. The trial court largely agreed with Target, ruling that most of the information sought by the plaintiffs was protected from discovery. Its order reveals the following strategies for prevailing on a future privilege claim to protect breach response.

- Lay the groundwork for the privilege claim in the initial stages of your breach response.
- Write on the face of all investigation material that it is privileged and was requested by counsel and prepared for legal advice.
- Make sure the originator of the material understands that it provides needed legal advice.
- Involve outside counsel from the beginning of the legal work.

Remember, legal privileges are never absolute. These strategies are intended to clarify a few points that often positively influence assertions of privilege, but they do not guaranty success. Keeping these approaches in mind at the outset of a breach response, or even including them in your practice breach response drills, is good to help ensure that your privilege defense remains fit throughout the chaos of a data breach.

In view of growing hacker activity and the high costs of dealing with data breaches, businesses should consider buying cyber insurance to cover expenses of complying with laws that require companies to notify customers and regulators when personal information has been compromised. Insurance usually covers costs of the following: liability (defense, legal fees, settlements, and judgments), forensic investigations, crisis management (public relations, breach notification and credit monitoring for victims), revenue loss from business interruptions, replacement of electronic data, repairing defaced websites, ransom payments to prevent damage from extortion, dealing with computer viruses, regulatory compliance, and director and officer liability.

Before buying insurance a business should have an attorney look at what is what is covered and what isn't. For example, a policy could be written such that the business may not be covered for employee-owned devices that could be the cause of the breach. This would have huge implications for its BYOD policies and protections.

The insurance should also cover expenses in dealing with computer viruses, and other cyber crimes. Businesses should also consider the following:

- Hire a computer security expert to evaluate your computers and website and suggest ways to protect them.
- Make sure your e-mail is secure by using a service provider that has proper security systems.
- Use another company to process credit card transactions. That company should guarantee that its systems are secure and use a service that helps to weed out fraudulent transactions.
- Encrypt names and data elements. Notice requirements are not triggered in this case.

If you provide credit monitoring and other identity protection services to you employees before or after a data breach, the value of those services will not be taxable to employees. And you need not include the value in the employees' gross income and wages, or report it on an information return such as a Form W-2 or Form 1099-MISC. See IRS Announcement 2015-22 for details.

DUE DILIGENCE WHEN BUYING OR MERGING WITH ANOTHER BUSINESS

Buying or merging with another business without analyzing how it protects its digital data could be as risky as buying a business without reviewing its financials. Cybersecurity should be an important part of the due-diligence process before acquisitions and mergers. The dangers of ignoring it have increased as data breaches become more common and many companies move their data offsite to a "cloud." Here are some questions that buyers should ask in its due diligence.

- What is your most sensitive data? Identify information such as trade secrets that hackers are most likely to target.
- Who is storing the data and where? Make sure that third parties who store the data have appropriate cybersecurity and cannot legally hold the data hostage in the event of a dispute.
- How is data protected from hackers? Cybersecurity experts should examine all aspects of the business' cybersecurity.
- How is data protected from internal leaks? Because rogue employees are the most likely source of data leaks, which employees have access to the data and what has the business done to prevent data leaks?
- Have there been past data breaches and how did the business handle them? What was done to prevent future breaches?

NEW YEAR'S RESOLUTIONS

Here is an example set of cybersecurity resolutions for your business to consider for the new year.

- Create or update your information-security and governance plans, and put them in writing.
- Update and test your plans annually. Include penetration testing along with a simulated data-breach event.
- Employee education should be your first priority. Individuals, not hackers, are the cause of most data breaches.
- Determine which business information is proprietary or sensitive information, confirm which employees need access to it, and then train those employees on keeping it secure. Also train them on safety in using the Internet of Things and the Internet.
- Use passwords that are at least 12 characters long, completely random, and have at least one capital letter, one lowercase letter, one number, and one symbol. Change them every 90 days. Easy-to-remember sentences or phrases make good passwords, such as "IlovetheLAChargers." Require employees to use a unique password for each system and service they use.
- Prohibit password sharing. It makes a hacker's job much easier.
- Complete regular software updates and patches. Most hacking events take advantage of old flaws that already have been addressed but proper patches have not been applied.
- Emphasize the importance of protecting your business and its customers when connecting to the Internet. Do not use public Wi-Fi except with an encrypted VPN.
- Become familiar with state and federal breach-notification laws. They can impact your business significantly.
- Determine if every employee or only those with access to proprietary or sensitive information need to have background checks. Effective pre-employment screening can help identify those who misrepresent themselves.
- Have every employee read and sign your information-security and governance plans annually.